WHITE PAPER

THREAT INTELLIGENCE PLATFORMS:

Open Source vs. Commercial

ThreatConnect™

ThreatConnect.com

Introduction

As a member of a maturing security team evaluating threat intelligence platforms (TIPs), you may be asking yourself whether you should use an open source solution like Malware Information Sharing Platform (MISP), or buy a TIP from one of many vendors offering solutions.

In this whitepaper, we discuss the key technical and economic considerations every security team needs to make when evaluating threat intelligence platform solutions, including service level agreements and integration with existing arrangements and legacy systems. And, importantly, which solution is right for your team.

"Why I Think I Need a TIP"

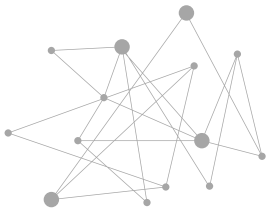
The first step to choosing the right TIP is figuring out what use cases are driving your need for the technology. A common pitfall that security teams make is that they approach the TIP selection process with a checklist of criteria, without really evaluating the problems they're trying to solve. As a result, they end up with a product that "checks all the boxes" but ends up collecting dust.

Spare us a moment as we use car buying as an analogy. If you're in the market for a new vehicle, some of the features you might look for are five star crash safety test ratings, a robust sound system, and decent gas mileage. These are all important qualities in a vehicle, but by focusing on features alone, you're ignoring the very reason why you're buying the car in the first place. Whether it's getting the kids to soccer practice on time, surviving the ultimate road trip out into the wilderness, or showing off your fancy new ride to the partners at your firm,the "features" listed above might all factor into these three "reasons," but imagine if the status-seeker showed up with a minivan, or the soccer parent showed up with a convertible coupe? The features are the same, but the final product, what's really needed, is totally different.

So, the first step in selecting a TIP – open source or otherwise – is not picking out the key features, it's nailing down the "job" of a TIP.

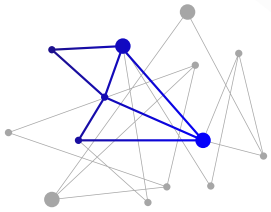
What's the job of a TIP?

Just as each person has a different motivation for choosing a car, every organization wants something different from their TIP, but for most teams the main jobs of a TIP are:



Aggregation:

The ability to centralize feeds and data into a single source of truth where they can be accessed in a standardized format by anyone who needs them.



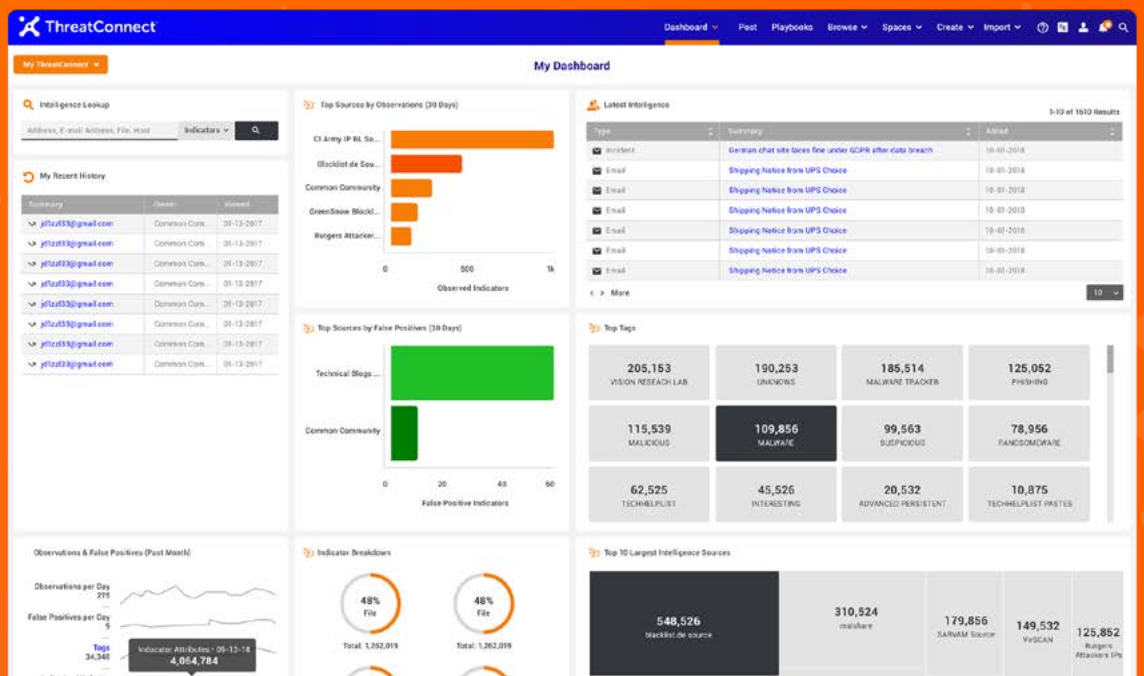
Analysis:

The ability to figure out what threats are relevant to you and your team.

Action:

Send the right intelligence to your detection and defense devices.

Major "check the box" items like DNS lookups, machine-readable threat intelligence, STIX/TAXII, etc., are all features in service of those larger goals. What matters, though, is how effectively the TIP can do the job you want it to do. You're probably doing those jobs today already with spreadsheets, cutting and pasting, Word docs, custom Python scripts, prayer, etc. The TIP makes you more effective at those jobs.



Choosing the Right TIP for the Job

Whatever use case(s) you have in mind for your TIP investment, finding one that checks all boxes isn't without its challenges. For example, if you're looking to centralize your data in one place a key obstacle to this desired state is that each of your threat feeds has a different format — STIX, CSVs, APIs, IP addresses, etc. If that's not enough, those formats shift frequently. Feed providers may change their APIs, what fields their bringing in, and so on. Centralizing that data into a common language requires a TIP that can adapt to these diverse and shifting formats.

Using a TIP to conduct threat analysis and determine which threats are relevant to you is also tricky. As with most cybersecurity activities, you're going to face a lot of noise. With millions of indicators feeding in each day, you need a TIP than can figure out which ones are relevant. Collaboration also becomes a challenge. With all that data being ingested and worked on by a growing yet disparate security team, how do you know who's responsible for what? Who's working on addressing which threats?

Validating your data and collaborating with your peers is crucial. When analysts work in a vacuum they quickly hit the end of the trail. An indicator may arise, but without collaboration and intelligence sharing, he or she can't know where to go next or what that indicator relates to.

What about sharing with management? Even the smallest teams usually have a leader or external stakeholder that needs to be updated regarding relevant security incidents or threats. If you don't have a central place for your data, or an easy way to present it to others, you will waste valuable hours gathering and compiling information on threats.

Finally, if you're looking to send the right intelligence to your detection and defense devices to optimize your SIEM, the same data challenges arise. Different defensive devices require data in conflicting formats, some use proprietary formats, some use STIX, others use an API.

Furthermore, these devices also require different data points and settings which warrants a specialized setup to get them to work with your TIP. And, of course, things break. Whether it's human error or a ghost in the machine, you need a TIP that's capable of monitoring defensive devices, as data is deployed to them, to ensure the intelligence that's being gathered and analyzed is doing what it's supposed to do.

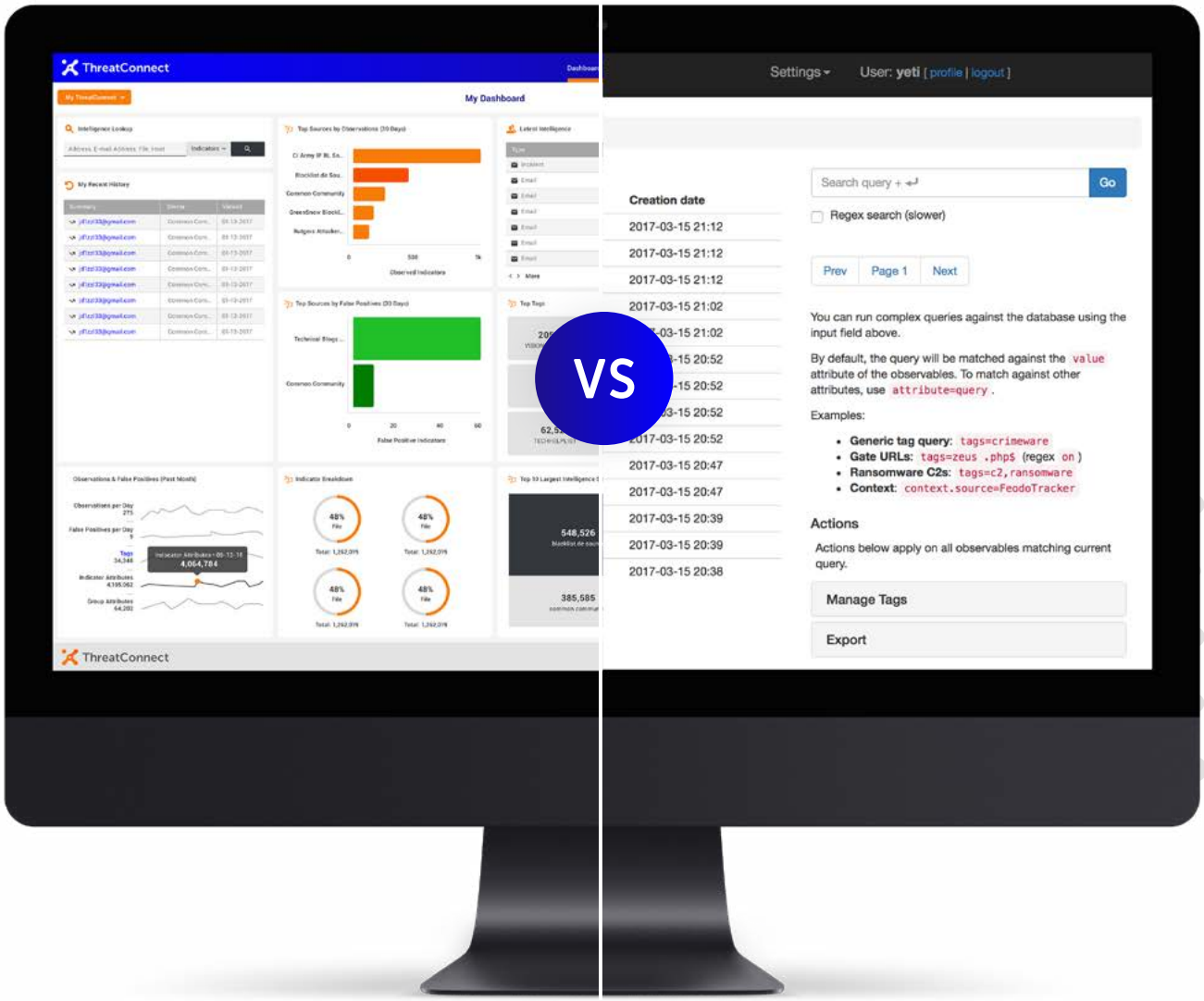
But which is right for your team? Which can accomplish the three key jobs of Aggregation, Analysis, and Action? Is it an open source or commercial TIP solution?

"...a commercial TIP that offers a security, orchestration, automation, and response (SOAR) capability natively integrated into that TIP's data model, like ThreatConnect, can let you automate tasks with minimal technical expertise for faster, more actionable insights..."

Making the Choice: Open Source VS. Commercial TIPs

There are many reasons why you might want to opt for an open source TIP, often this comes down to perceived ideas about cost. But regardless of the payment structure, you can expect to pay significantly more for an open source solution over time while sacrificing many of the features that you're looking for to support the "job" of your TIP.

Let's break them down:



The Hidden Costs of Open Source

The cost of commercial TIPs can often be viewed as a big hurdle when selecting and investing funds. It's true that open source solutions have a lower cost of entry, but the long-term support costs can add-up and nullify any initial cost investment benefits. Why is that? To support your open source TIP, you can either turn to in-house or contracted resources, or you can turn to the open source community-usually through a TIP's help forum, knowledge base, or wiki. This can be costly in the long-run for several reasons.

First, the open source TIP community develops solutions based on its own challenges, which may not be the same as yours. For example, wikis are intended to provide support based on the specific jobs that the wiki creators implemented their TIP to do. These are likely to be at odds with what your team uses a TIP for.

Ironically, the open source community also opens a Pandora's Box when it comes to the issue of security. Each time you post a question or a problem related to an open source TIP, you'll need to reference your infrastructure or the tools you use in a public way through community chat and forums, potentially exposing your organization to risk.

The difference extends beyond cost and support to the very DNA of the TIP. Typically, a commercial TIP is built with a purpose in mind – it's designed to do something. This stands in contrast to one of the key characteristics of any open source solution which is open-endedness. Open source options are produced as collaborative efforts and can fall victim to a "too many cooks in the kitchen" scenario. This makes it harder to determine if that TIP checks each box on your shopping list.

At their core, commercial TIPs leverage a wide-range of expertise — geopolitical, analytical, and engineering – in a strategic and organized way. With this know-how built-in, as opposed to community-contributed, it becomes much easier to gauge how effectively the TIP can do the job you want it to do.

What About Customization?

When choosing a TIP, customization is key. As you move up the threat intelligence maturity model, chances are you'll want to do more things with your TIP. Beyond reporting to both your threat detection and incident response teams, you may want to add more strategic reporting capabilities so that your CISO can report on ROI to prove the effectiveness of your threat intelligence program and inform board-level decision making. Customizing this level of reporting is where open source and commercial platforms diverge significantly.

Open source, with its inherent ability to be freely distributed and modified, can seem like the perfect fit for such customization. It actually isn't a question of which platform is more customizable, but whether your organization has the skills and resources to handle this customization in a timely manner. Tailoring an open source TIP may require so much coding and development that, at the end of the day, you've built your own bespoke (and costly) TIP.

Commercial solutions vary widely in their level of customization. Some may require a steep learning curve, but the best solutions will be designed in a way that they can be easily customized in all the right areas. They give you the ability to add to the data model, to customize how the TIP works, and tailor the kind of data included in the platform for reporting purposes. This idea of an extensible data model caters to the different needs across your organization and delivers the right data points, whether you're a threat analyst, incident responder, or CISO.

To reiterate, it comes down to not which platform is more customizable, but whether your team can customize one more effectively than the other.

Overcoming Training Challenges

Another important consideration to choosing open source or commercial TIP is training. Any TIP solution requires a level of expertise. When approaching any TIP implementation, your security team must have a handle on its processes, priorities, and objectives, as well as how much work it's willing to do upfront.

If you go the open source route, you'll need to hire new engineers to help you tailor that TIP to meet your precise needs and processes – a process that can take several months. This can result in additional labor costs, but, once the TIP is turned over to your security team, the ramp-up window should be quick since the system was developed in close collaboration with your security team.

If you choose a commercial TIP, be prepared to expect an initial ramp-up period as your team familiarizes themselves with a new process. The good news is you're not alone. Proprietary solutions provide dedicated documentation and support tools tailored to your enterprise. Furthermore, a TIP like ThreatConnect gives you access to a customer success manager who'll work one-on-one with your team to understand your processes and priorities and help you get most value out of the TIP – all bundled as part of the purchase.

Integration with Legacy Systems

Integration is a perpetual challenge for any new technology purchase. How do commercial versus open source TIPs stack up?

Here the challenge of handling legacy feeds characterized by different formats and protocols comes sharply into focus. Any open source TIP will require hefty modification and support maintenance costs to ensure it can ingest those legacy feeds. A commercial TIP, however, comes to you with integration options for numerous open source and premium paid feeds due to an extensive ability to ingest multiple types of data presented in various formats.

As you review your wish list for a TIP, if your main goal is to centralize all your feeds in one place, choosing an open source solution prohibits your ability to feed in different and constantly changing data formats. By comparison, ThreatConnect has an entire team dedicated to managing those shifting changes and keeping each integration up-to-date and working as intended.

Cost also comes into play. It's not simply a question of support that drives up the cost of open source over time, but the expense of keeping that solution up-to-date with all the technologies you've integrated it with. This is, after all, one goal of a TIP – getting all of your security solutions to a point where they can benefit from threat intelligence

Automation and Orchestration

Since we've discussed heavy-lifting as a key challenge of any open source TIP solution, a natural progression leads to the question of automation and orchestration and which medium handles this capability best, open source or commercial?

It all depends once more on what your goals and use cases are. What do you want to automate? If an analyst is spending their day cutting and pasting between different tools or manually uploading malware files to a sandbox for testing – are these things that could be automated?

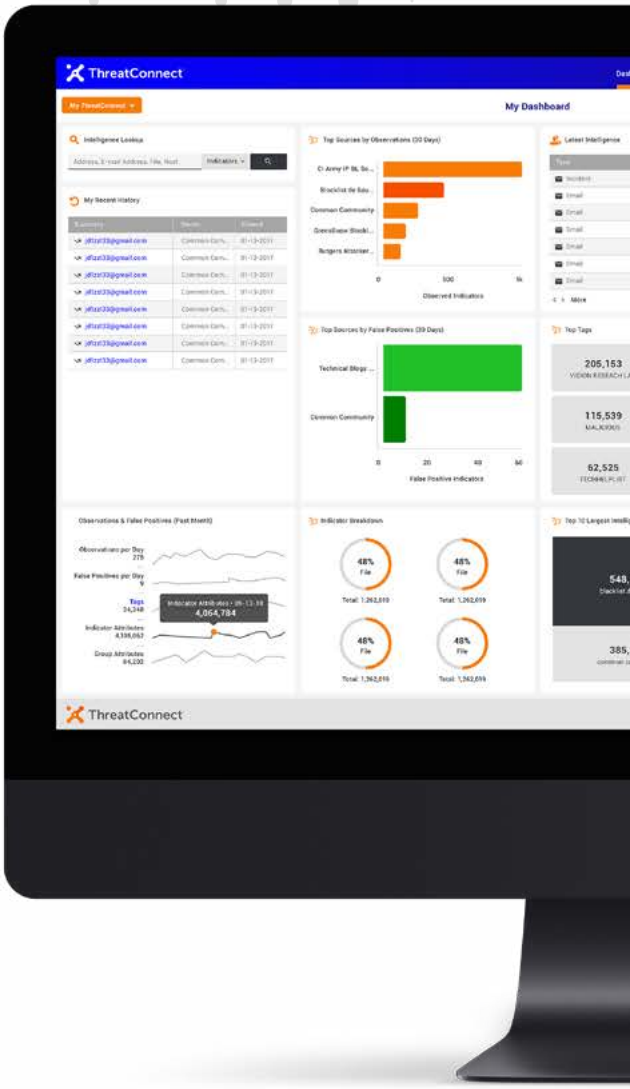
Dedicated automation capabilities cannot be found in today's open source marketplace. However, they may offer scripting capabilities, which requires coding resources and possibly hiring yet more developers.

On the other hand, a commercial TIP that offers a security, orchestration, automation, and response (SOAR) capability natively integrated into that TIP's data model, like ThreatConnect, can let you automate tasks with minimal technical expertise for faster, more actionable insights than you could with an open source offering.

Conclusion

While lower upfront costs make open source TIPs an attractive proposition, the long-term outlays, and customization, integration, and training challenges may make you think twice.

Ultimately, it's a question of requirements. How much time and effort can you afford to spend on an open source TIP? Would you be better served with a solution that has much of the functionality you need out-of-the-box and fully supported? There's no black or white answer. In the end, when we talk about selecting a TIP based on what your organization needs it to do, keep these things in mind:



- ✓ **Make a checklist of what you and your team need the TIP to aggregate, analyze, and operationalize. Don't rely on a wish list of features, rely on the jobs you want done.**
- ✓ **For each item on the list, consider how it's being done now.**
- ✓ **For every TIP you're evaluating, consider how that TIP accomplishes the jobs on your checklist.**
- ✓ **Remember that orchestration is just another way to accomplish one of those jobs.**

ThreatConnect

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit ThreatConnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708